CLAIMS

We Claim:

1. A method for securely exchanging information items used to generate encryption keys among at least two parties using a public/private encryption key system over a communication network, each of said parties retaining an initial private key and transmitting an initial corresponding information item used by each receiving party to determine, and retain, an initial encryption key, said method comprising the steps of:

a. determining a next private key and a next corresponding information item set, wherein said next private key is retained among said retained next private keys;

b. encrypting at least one element of said next information item using an encryption key selected from said retained encryption keys;

c. transmitting said next information item over said network;

d. decrypting a received encrypted information item element using a private key selected from said retained private keys; and

e. determining a next encryption key from said next private key and said received information item, wherein said next encryption key is retained among said retained encryption keys.

2. The method as recited in Claim 1 wherein

steps a-e are repeated until a known number of encryption keys are determined.

3. The method as recited in claim 1 wherein said information item element is a public key.

4. The method as recited in claim 1 wherein said information item element is a synchronizing indicator.

5. The method as recited in claim 1 wherein the step of encrypting further comprises:

selecting at least one of said retained encryption keys alternatively.

6. The method as recited in claim 1, wherein the step of encrypting further comprises:

selecting a known encryption key.

7. The method as recited in claim 6 wherein said known encryption key is such that an output value is the same as an input value.

8. The method as recited in claim 5 wherein said encryption keys are selected in a known sequence.

9. The method as recited in claim 8 wherein said known sequence corresponds to an order of retention of said encryption keys.

10. The method as recited in claim 8 wherein said known sequence corresponds to an order pre-selected by said parties.

11. A system for securely exchanging information items used to generate encryption keys among at least two parties using a public/private encryption key system over a

communication network, each of said parties retaining an initial private key in a memory and transmitting an initial corresponding information item used by each receiving party to determine, and retain in said memory, an initial encryption key, said system comprising:

a receiving device operative to receive a plurality of information items over said network;

a processor in communication with said memory operative to:

determine at least one next private key and at least one next corresponding information item set, wherein said at least one next private key is retained in said memory;

encrypt at least one element of each of said at least one next information item using an encryption key selected from encryption keys retained in said memory;

decrypt each of at least one received encrypted information item element using a private key selected from said private keys retained in said memory; and

determine at least one next encryption key from corresponding said at least one next private key and said at least one received information item, wherein said at least one next encryption key is retained in said memory; and

a transmitting device operative to transmit each of said at least one information items.

12. The system as recited in claim 11 wherein said information item element is a public key.

13. The system as recited in claim 11 wherein said information item element is a synchronizing indicator.

14. The system as recited in claim 11 wherein said processor is further operative to alternatively select at least one of said at least one retained next encryption key.

15. The system as recited in claim 11, wherein said processor is further operative to select a known encryption key.

16. The system as recited in claim 11 wherein said known encryption key renders an output value the same as an input value.

17. The system as recited in claim 14 wherein said encryption keys are selected in a known sequence.

18. The system as recited in claim 17 wherein said encryption keys are selected in a known order determined by said parties.

19. The system as recited in claim 17 wherein said known sequence corresponds to an order of retaining each of said next encryption keys in said memory.

20. A device for securely exchanging information items used to generate encryption keys among at least two parties using a public/private encryption key system over a

communication network, each of said parties retaining an initial private key in a memory and transmitting an initial corresponding information item used by each receiving party to determine, and retain in said memory, an initial encryption key, said device, in communication with a receiving device and a transmitting device, comprising:

a key generator to generate a next private key and a next information item, wherein said next private key is stored in said memory in communication with said key generator;

an encryption device operative to encrypt at least one element of said next information item using an encryption key selected from encryption keys retained in said memory and communicate said next information item to said transmitting device;

a decrypting device to operative to receive information item from said receiving device and decrypt said received information item element using a private key selected from said private keys retained in said memory ;and

an encryption key generator to determine a next encryption key from corresponding said next private key and said received information item, wherein next encryption key is retained in said memory; and

21. The device as recited in claim 20 wherein said next information item element is a public key.

22. The device as recited in claim 20 wherein said next information item element is a synchronizing indicator.

23. The device as recited in claim 20 wherein said encryption device is further operative to:

alternatively select at least one of said retained encryption keys.

24. The device as recited in claim 20, wherein said encryption device is further operative to select a known encryption key.

25. The device as recited in claim 24 wherein said known encryption key is such that an output value is the same as an input value.

26. The device as recited in claim 23 wherein said encryption device is operative to select said encryption keys in a known sequence.

27. The device as recited in claim 26 wherein said known sequence corresponds to an order said encryption keys are retained in said memory.

28. The device as recited in claim 26 wherein said known sequence corresponds to a pre-determined order established between said parties.